인공지능 보안

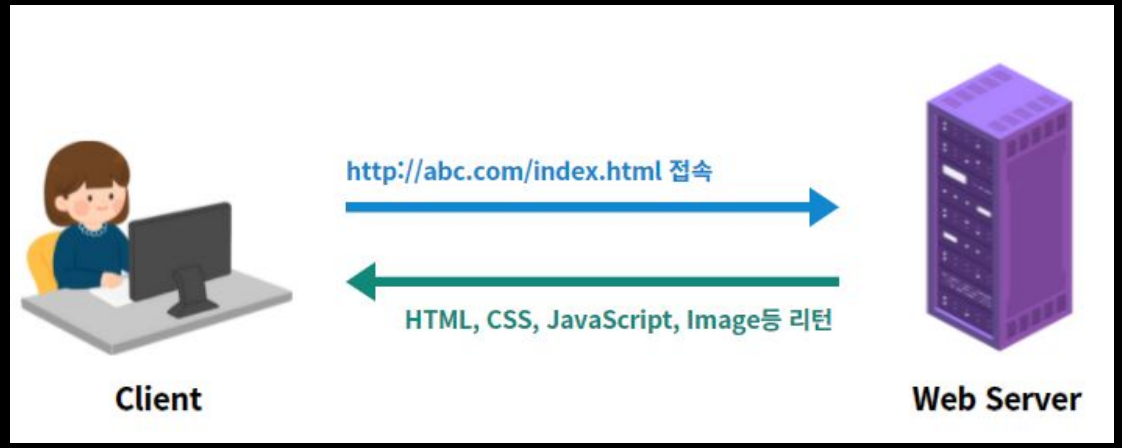
-11-

웹 보안

HTTP

HTTP (HyperText Transfer Protocol)

- 웹에서 가장 많이 쓰이는 프로토콜은 HTTP
- HTTP는 웹 처리 전반에 걸친 토대가 되기 때문에 웹 서버를 HTTP 서버라고 부르기도 함



- 연결 과정
  - 클라이언트는 읽고자 하는 문서를 서버에 요청
  - 서버는 웹 문서 중에서 요청받은 것을 클라이언트에 전송

HTTP Request

- GET 방식
  - 가장 일반적인 HTTP Request 형태로, 요청 데이터 값을 웹 브라우저의 URL로 전송
  - 데이터가 주소 입력란에 표시되므로 최소한의 보안도 유지되지 않는 취약한 방식

- POST 방식
  - URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송.
  - 값을 URL로 전송하지 않으므로 다른 사용자가 링크로 해당 페이지를 볼 수 없음
  - 게시판의 경우, 목록이나 글 보기 화면은 접근 자유도를 위해 GET 방식을 사용
  - 게시글을 저장·수정·삭제하거나 대용량 데이터를 전송할 때는 POST 방식을 사용

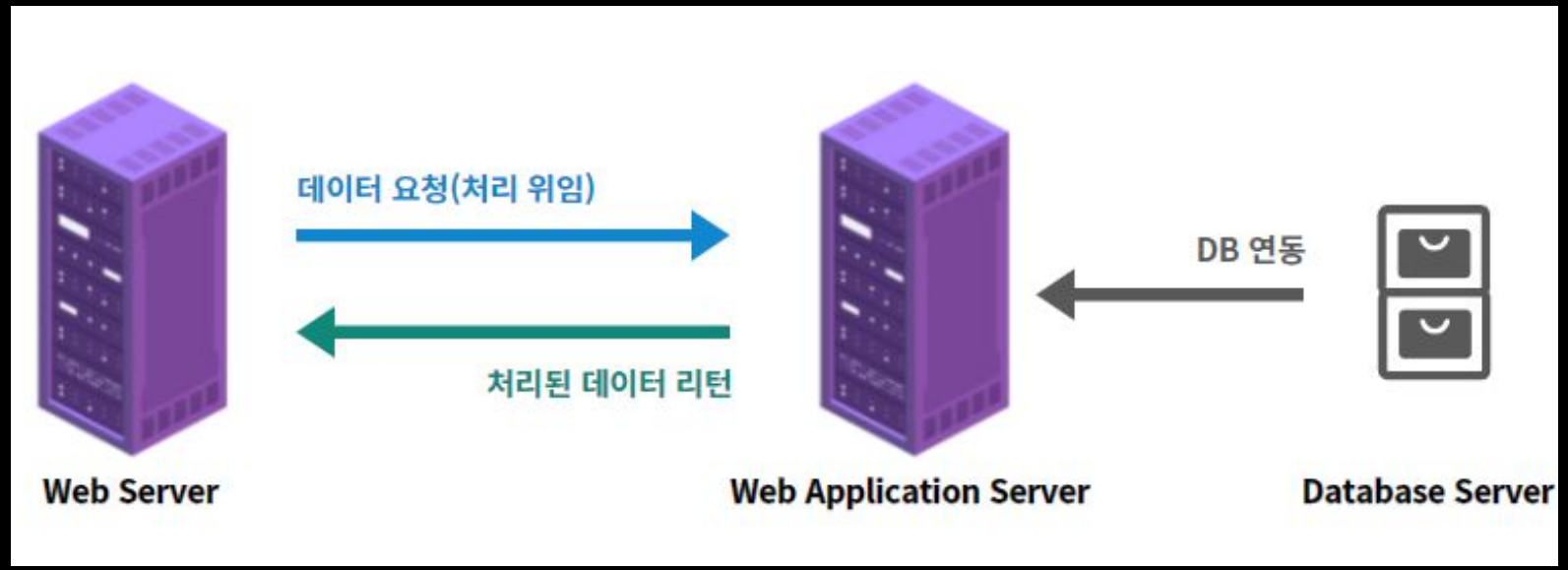
- 기타 방식
  - HEAD, OPTIONS, PUT, DELETE, TRACE

HTTP Response

- 클라이언트의 HTTP Request에 대한 응답 패킷
- 서버에서 쓰이는 프로토콜 버전, Request에 대한 실행 결과 코드, 간략한 실행 결과 설명문 내용이 담겨 있음
- 헤더 정보 뒤에는 실제 데이터(HTML 또는 이미지 파일 등)이 전달됨

실행 결과 코드	내용	설명
100번대	정보 전송	HTTP 1.0까지는 계열에 대한 정의가 이루어지지 않았기 때문에 실험 용도 외에는 100번대 서버 측의 응답이 없다.
200번대	성공	클라이언트의 요구가 성공적으로 수신 및 처리되었음을 의미한다.
300번대	리다이렉션	해당 요구 사항을 처리하기 위해 사용자 에이전트가 수행해야 할 추가 동작이 있음을 의미한다.
400번대	클라이언트 측 에러	클라이언트에 오류가 발생했을 때 사용한다. 예를 들면 클라이언트가 서버에 보내는 요구 메시지를 완전히 처리하지 못한 경우 등이다.
500번대	서버 측 에러	서버 자체에서 발생한 오류 상황이나 요구 사항을 제대로 처리할 수 없을 때 사용한다.

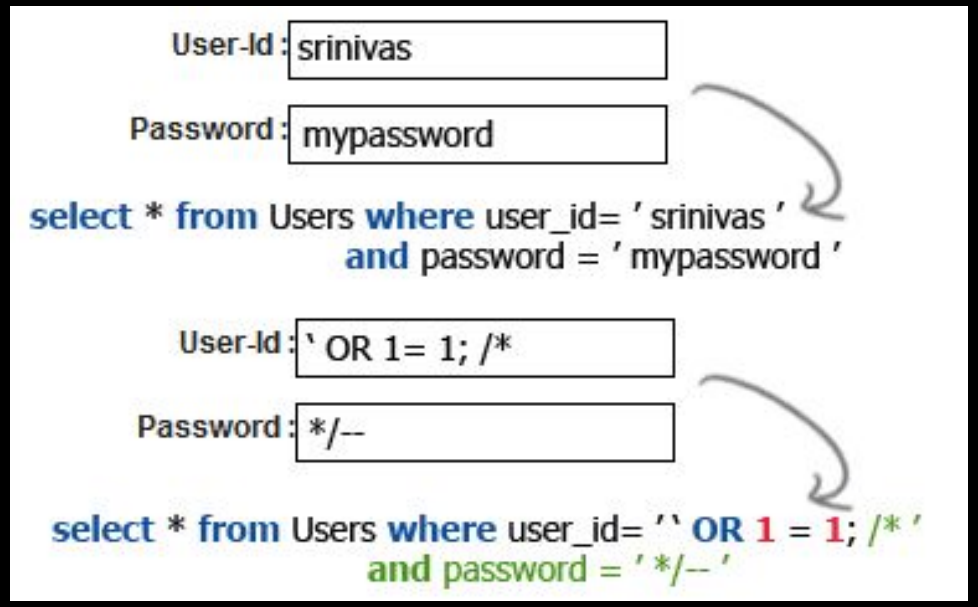
WEB-WAS-DB


데이터 요청(처리 위임)
처리된 데이터 리턴
DB 연동
Web Server
Web Application Server
Database Server

웹 서비스 취약점 공격

SQL Injection

악의적인 SQL문을 실행되게 함으로써 데이터베이스를 조작

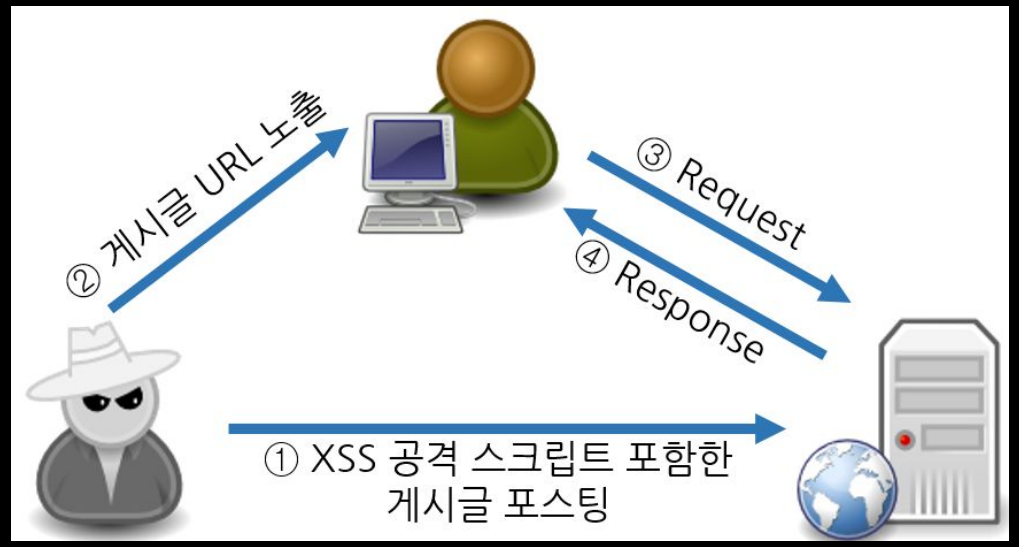


사용자의 입력이 SQL문에 동적으로 영향을 주는 경우, 입력된 값이 개발자가 의도한 값인지 검증하고 차단

/*, -, ‘, “, ?, #, (,), ;, @, =, *, +, union, select, drop, update, from, where, join, substr, user_tables, user_table_columns, information_schema, sysobject, table_schema, declare, dual,…

XSS (Cross Site Scripting)

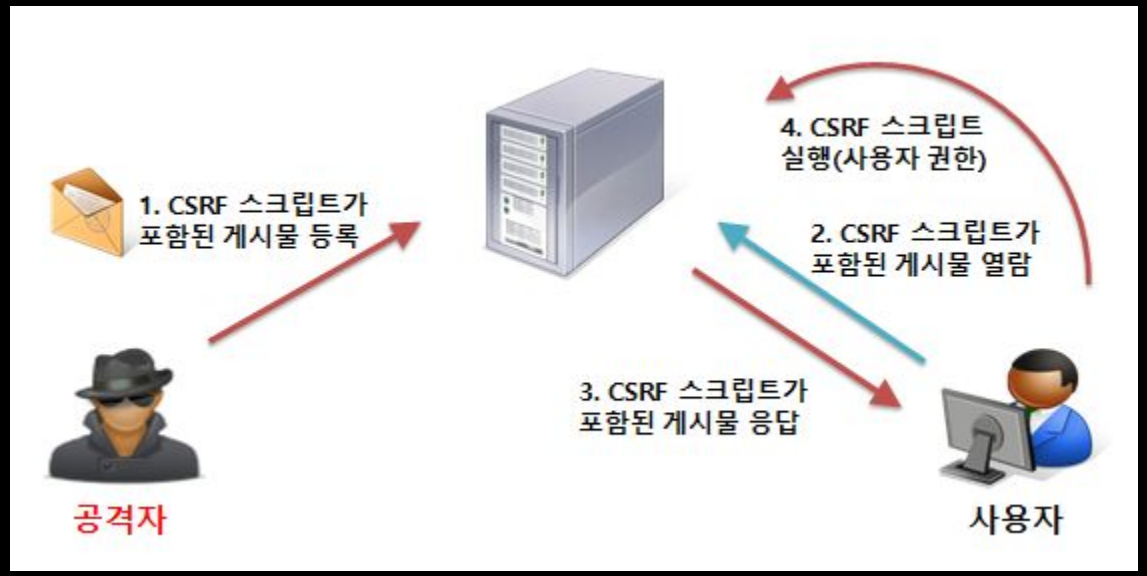
웹 페이지에 악성 스크립트를 삽입하는 방식으로 이루어지는 공격
쿠키, 세션ID 탈취, 악성 코드 다운로드 등



스크립트 태그에 자주 사용되는 <, > 등 과 같은 문자를 필터링 해주는 방법으로 방어

CSRF (Cross Site Request Forgery)

사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)을 특정 웹사이트에 요청하게 하는 공격



XSS(Cross Site Script) 스크립트의 실행 방지, Referer 필드 확인

Broken Access Control

취약한 접근 제어
인증된 사용자가 수행할 수 있는 것에 대한 제한을 제대로 적용하지 않은 것

정상적인 다운로드 페이지를 이용하여 다른 파일의 다운로드를 요청

http://www.xxx.com/board/download.jsp?filename=../list.jsp

인증 로직을 만들어 웹에 존재하는 모든 페이지의 앞부분에 입력

Q&A